

Secret Sharing

Henning Hontheim

10. März 2020

Inhaltsverzeichnis

1	Wozu Secret Sharing?	1
1.1	Ein kombinatorisches Beispiel	1
2	Primitives Secret Sharing	2
2.1	Aufsplitten des Secrets	2
2.2	One-Time-Padding	2
	Vernam-Chiffre	2
	Visuelle Kryptographie	3
	One-Time-Padding mit mehr als 2 Personen	5
3	Shamir's Secret Sharing	5
3.1	Das Shamir-Secret-Sharing-Protokoll	6
3.2	Berechnen der Shares	8
3.3	Rekonstruktion des Geheimnisses	8
3.4	Sicherheit	8
3.5	Beispiele	8
	Graphisches $(2, n)$ -Schema	8
	Graphisches $(3, n)$ -Schema	8
4	Weitere Verfahren	9
4.1	Blakeley's	9
4.2	Chinesischer Restsatz	9
4.3	whatever...	9
5	Fazit	10
	Abbildungsverzeichnis	11
	Literaturverzeichnis	11

Allein aus Gründen der Lesbarkeit wird auf die gleichzeitige Verwendung mehrerer geschlechtsspezifischer Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter.

1 Wozu Secret Sharing?

Arbeiten Sie mit Anderen an einem geheimen Projekt, so gibt es einige Herausforderungen zu meistern. Was passiert, wenn Sie Ihren Schlüssel der verschlüsselten Daten verlieren? Haben lediglich Sie einen Schlüssel? Wahrscheinlich nicht. Es ist nützlich, seien es in einem Tresor verschlüsselte Daten, oder die privaten Schlüssel in einer PKI, wenn nicht nur Sie den einzigen Schlüssel besitzen.

Aber wie teilen Sie den Zugriff auf die Daten? Wenn Sie Ihren Schlüssel vervielfältigen würden, hätte ein Einzelner Vollzugriff. Es wäre besser, wenn es mehrere Personen benötigen würde, um Zugriff zu erhalten – idealerweise mehr als die Hälfte aller Beteiligten. Doch wie lässt es sich in der Praxis umsetzen, dass es mehrere Personen benötigt um einen privaten Schlüssel zu rekonstruieren?

Ich möchte hier eine Technik vorstellen, die es erlaubt, Geheimnisse mit anderen zu teilen – das Secret Sharing. Siehe [1] und [5].

1.1 Ein kombinatorisches Beispiel

Mehrere Wissenschaftler N arbeiten zusammen an einem Geheimprojekt. Um die Dokumente geheim zu halten und um Missbrauch vorzubeugen, verschließen sie diese in einem Tresor. Nur wenn mindestens die Hälfte aller Wissenschaftler anwesend ist, soll sich der Tresor öffnen lassen. Wie viele paarweise verschiedene Schlösser S muss der Tresor mindestens besitzen? Wie viele paarweise verschiedene Schlüssel s muss jeder Wissenschaftler mindestens bei sich tragen? Siehe [5] nach [3].

Beispiel 1.1. Sei $N = 11$ die Anzahl aller Wissenschaftler und $n = \lceil \frac{N}{2} \rceil = 6$ die Anzahl derer, die mindestens anwesend sein müssen, damit sich der Tresor öffnen lässt. Folglich muss es also für jede Teilmenge mit k Wissenschaftlern, wobei $k = N - n = 5$, genau ein Schloss geben, für das keiner der k Wissenschaftler einen Schlüssel besitzt. Also muss der Tresor $S = \binom{N}{k} = \binom{11}{5} = 462$ paarweise verschiedene Schlösser besitzen.

Sei $W = \{w_1, w_2, \dots, w_k, w_{k+1}\}$ mit $|W| = k + 1 = 6$ die Menge von Wissenschaftlern, die mindestens benötigt wird, um den Tresor zu öffnen. Dann gibt es genau ein bestimmtes Schloss S' , für das keiner der Wissenschaftler aus $W \setminus w_{k+1}$ einen Schlüssel besitzt, der Wissenschaftler w_{k+1} jedoch schon. Da für jede Permutation von $k = 5$ Wissenschaftlern genau der w_{k+1} existiert, der die Teilmenge W „vervollständigt“, bekommt jeder Wissenschaftler $s = \binom{N-1}{|W|-1} = \binom{N-1}{k} = \binom{10}{5} = 252$ Schlüssel. Das ergibt eine Gesamtanzahl an $11 \cdot 252 = 2772$ Schlüsseln. Dass dies keine praktikable Lösung des Problems ist, ist offensichtlich.

2 Primitives Secret Sharing

2.1 Aufsplitten des Secrets

Ein primitives Vorgehen zur Aufteilung eines Geheimnisses wäre es, dieses nach einer gewissen Anzahl Stellen zu trennen.

Beispiel 2.1. Sei $D = 14561237$ das Geheimnis, welchen unter 2 Personen aufgeteilt werden soll. Bei 8 Stellen, könnte man der ersten Person P_1 die ersten 4 Stellen, der zweiten Person P_2 die letzten 4 Stellen zuteilen.

$$D = 14561237 = \underbrace{1456}_{=:D_1} \underbrace{1237}_{=:D_2} = D_1 \cdot 10^4 + D_2$$

Der entscheidende Nachteil hierbei ist, dass die Shares¹ D_1 und D_2 Aufschluss über die Beschaffenheit von D geben. Wer D_1 besitzt braucht nur 10^4 Kombinationen zu testen, wohingegen ein unbeteiligter Dritter 10^8 ausprobieren müsste.

Fortan fordern wir also, dass es eine wichtige Eigenschaft der Shares sein muss, keine Informationen über das Geheimnis D preiszugeben und alle Möglichkeiten von D gleich wahrscheinlich sein sollen. Dies wird beschrieben durch das Prinzip der Konfusion, welches auf den Mathematiker Claude Shannon zurückzuführen ist.[6]

2.2 One-Time-Padding

Vernam-Chiffre

Ein Verfahren, welches die geforderte Eigenschaft nicht verletzt, ist das sogenannte One-Time-Padding. Dieses beruht auf der Vernam-Chiffre. Hierbei wird eine zufällige Zahl r zu unserem Geheimnis D addiert, wobei beide die gleiche Stellenanzahl haben müssen.

Beispiel 2.2. Sei wieder $D = 14561237$ und ein $r_1 = 81613241$ zufällig gewählt. Nun berechnen wir $r_2 = D \oplus r_1$, wobei wir hier \oplus die Addition modulo 10 ist, die Überträge also quasi vernachlässigt werden. Hier wäre beispielsweise $5 \oplus 6 = 1$.

$$\begin{array}{rcl} 14561237 & = & D \\ \oplus & 81613241 & = r_1 \\ \hline 95174478 & = & r_2 \end{array} \tag{1}$$

¹Shares sind die Bestandteile eines Geheimnisses, die zur Rekonstruktion dessen an die beteiligten Personen aufgeteilt werden

Nun können wir das Geheimnis rekonstruieren, wenn wir $D = r_2 \ominus r_1$ stellenweise rechnen. Unsere Subtraktion \ominus wird wieder modulo 10 gerechnet, ignoriert also auch hier für jede Stelle den (negativen) Übertrag. Somit wäre beispielsweise $1 \ominus 6 = +5$.

$$\begin{array}{rcl} 95174478 & = & r_2 \\ \ominus & 81613241 & = r_1 \\ \hline 14561237 & = & D \end{array} \quad (2)$$

Wenn wir nun zwei Personen haben, die D unter sich aufteilen möchten, erhält P_1 den Share $r_1 = 81613241$ und P_2 den Share $r_2 = 95174478$. Beide Shares geben keinerlei Aufschluss über die Beschaffenheit von D . Zusammen können P_1 und P_2 das Geheimnis jedoch rekonstruieren.

Es soll angemerkt sein, dass die Addition modulo 10 nur eine mehrerer Möglichkeiten der Berechnung ist. Handelt es sich um binäre Zahlen liegt es nahe, die XOR²-Operation zu nutzen.

Visuelle Kryptographie

Ein weiteres anschauliches Beispiel lässt sich im Bereich der Visuellen Kryptographie finden. Hier besteht das Geheimnis (Abbildung 4) aus einer s/w-Grafik. Diese Grafik wird aufgeteilt und jeder Teil auf eine transparente Folie gedruckt. Wenn nun die Folien übereinandergelegt werden, erscheint die ursprüngliche Grafik. Jede einzelne Folie sieht dabei wie ein zufälliges Rauschen gleichverteilter schwarzer und weißer Pixel aus. Siehe [4].

Beispiel 2.3. Ein Bild soll auf zwei Folien aufgeteilt werden. Die erste Folie (Abbildung 1) wird mit einem zufälligen Muster bedruckt. Aus Gründen des Kontrasts müssen für jedes Pixel des originalen Bildes 4 Pixel (je ein 2×2 -Quadrat) generiert werden. Die Folien enthalten also alle viermal so viele Pixel. Hierbei werden für jedes Quadrats entweder die beiden Sub-Pixel oben links und unten rechts, oder die anderen beiden Sub-Pixel oben rechts und unten links schwarz eingefärbt.

²Exklusiv-Oder



Abbildung 1: Eine zufällige erste Folie. Von [2].

Die Pixel der zweiten Folie (Abbildung 3) werden gemäß Abbildung 2 berechnet. Wenn im Original ein schwarzes Pixel (■) vorhanden ist, muss an dieser Stelle in der zweiten Folie das Komplement der ersten Folie eingefärbt werden. Somit sind bei Überlagerung beider Folien alle 4 Sub-Pixel schwarz. Wenn das originale Pixel weiß ist (□), hat das Quadrat der zweiten Folie das gleiche Muster wie die erste Folie. Das ergibt in Summe ein graues Pixel (#7F7F7F). Weiße Pixel können über Folien nicht rekonstruiert werden, da mit den Folien keine Subtraktion möglich ist. Deshalb muss die Pixelanzahl auch vervierfacht werden. Siehe [2].

Zufallsbitsstrom aus Zufallszahlengenerator: 01010010010101100111...

Zufallsbit:	0	1	0	1
Pixel Folie 1: (folgt Zufallsbit)				
Ursprungspixel:				
Pixel Folie 2: (abgestimmt auf Ergebnis)				
Überlagerung Folie 1 und 2 (~ Ursprungspixel)				

Abbildung 2: Berechnung der Pixel der zweiten Folie. Von [2].



Abbildung 3: Die zweite Folie. Von [2].

Wenn nun beide Folien übereinandergelegt werden, erscheint das Geheimnis:



Abbildung 4: Das mittels beider Folien rekonstruierte Geheimnis. Von [2].

One-Time-Padding mit mehr als 2 Personen

Wie sieht es jedoch aus, wenn sich mehr als zwei Personen ein Geheimnis mittels OTP³ teilen möchten? Auch dies ist möglich für eine beliebige Anzahl N an Personen. Doch was passiert, wenn einer der Beteiligten den eigenen Share verliert? Da alle Shares benötigt werden um D zu rekonstruieren, ist das unser SPOF⁴. Da dies in der Praxis für große N sehr schnell zu einem Problem führen kann, möchten wir dieses Verfahren hier nicht länger behandeln.

3 Shamir's Secret Sharing

Wir widmen uns nun einem Verfahren mit dem sich ein Geheimnis rekonstruieren lässt, ohne dass alle Shares benötigt sind. Wie im Beispiel mit den Schlössern wollen wir einen Schwellwert von Shares angeben, die mindestens zur Rekonstruktion des Geheimnisses benötigt sein sollen. Das hier vorgestellte Secret-Sharing-Protokoll stammt von Adi Shamir. [5]

³One-Time-Padding

⁴Single Point of Failure

Seien $n, t \in \mathbb{N}$ mit $t \leq n$. Bei diesem (n, t) -Secret-Sharing-Protokoll wird das Geheimnis von einem Dealer auf n Personen aufgeteilt. Jeder hat einen Teil des Geheimnisses. Wenn sich t dieser Personen zusammentun, sollen sie das Geheimnis rekonstruieren können. Wenn sich aber weniger als t dieser Geheimnisträger zusammentun, sollen sie keine relevante Information über das Geheimnis erhalten können. [1]

3.1 Das Shamir-Secret-Sharing-Protokoll

Bevor wir mit der Beschreibung des Protokolls beginnen können, beschäftigen wir uns mit *Vandermonde*⁵-Matrizen.

Definition 3.1. Eine Vandermonde-Matrix V_n ist eine $(n \times n)$ -Matrix der Form

$$V_n = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}.$$

Hierbei gilt $V_n = V(a_1, \dots, a_n) := (v_{ij})$ mit $v_{ij} := a_i^{(j-1)}$ für $1 \leq i, j \leq n$.

Lemma 3.2. Die Determinante einer Vandermonde-Matrix V_n ist

$$\det V_n = \prod_{1 \leq j < i \leq n} (a_i - a_j).$$

Beweis. Wir beweisen dies mithilfe vollständiger Induktion. Den trivialen Fall für $\det V_1 = \det(1) = 1$ vernachlässigen wir hierbei.

- **Induktionsanfang $n = 2$:**

Der Induktionsanfang für $n = 2$ ist schnell gezeigt:

$$\det(V_2) = \det \begin{pmatrix} 1 & a_1 \\ 1 & a_2 \end{pmatrix} = 1 \cdot a_2 - 1 \cdot a_1 = \prod_{j=1, i=2} (a_i - a_j) = \prod_{1 \leq j < i \leq 2} (a_i - a_j).$$

- **Induktionsschritt $n - 1 \rightarrow n$:**

ladida

□

⁵nach Alexandre-Théophile Vandermonde

Satz 3.3. Seien $l, t \in \mathbb{N}, l \leq t$. Weiter seien $x_i, y_i \in \mathbb{Z}/p\mathbb{Z}, 1 \leq i \leq l$, wobei die x_i paarweise verschieden sind. Dann gibt es genau p^{t-l} Polynome $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ vom Grad $\leq t-1$ mit $b(x_i) = y_i, 1 \leq i \leq l$.⁶

Beweis. Das Lagrange-Interpolationsverfahren liefert das Polynom

$$b(x) = \sum_{i=1}^l y_i \prod_{j=1, j \neq i}^l \frac{x_j - X}{x_j - x_i}, \quad (3)$$

das $b(x_i) = y_i, 1 \leq i \leq l$ erfüllt und mit dem sich b wieder interpolieren lässt. Jetzt muss nur noch die Anzahl dieser Polynome bestimmt werden.

Sei $b \in (\mathbb{Z}/p\mathbb{Z})[X]$ ein solches Polynom. Dieses lässt sich wie folgt darstellen:

$$b(x) = \sum_{j=0}^{t-1} b_j X^j, b_j \in \mathbb{Z}/p\mathbb{Z}, 0 \leq j \leq t-1.$$

Aus $b(x_i) = y_i, 1 \leq i \leq l$ erhält man das lineare Gleichungssystem

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^{t-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_l \end{pmatrix}. \quad (4)$$

Die Teil-Koeffizientenmatrix

$$U = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{l-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{l-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_l & x_l^2 & \cdots & x_l^{l-1} \end{pmatrix}$$

ist eine *Vandermonde-Matrix*. Ihre Determinante ist

$$\det U = \prod_{1 \leq i < j \leq l} (x_j - x_i).$$

Weil die x_i nach Voraussetzung paarweise verschieden sind, ist die Determinante ungleich Null. Der Rang von U ist also l . Daher hat der Kern der Koeffizientenmatrix des linearen Gleichungssystems (4) den Rang $t-l$ und die Anzahl der Lösungen ist p^{t-l} . \square

⁶In unserem konkreten Fall gilt $l = t$.

3.2 Berechnen der Shares

3.3 Rekonstruktion des Geheimnisses

3.4 Sicherheit

3.5 Beispiele

Graphisches $(2, n)$ -Schema

Blah

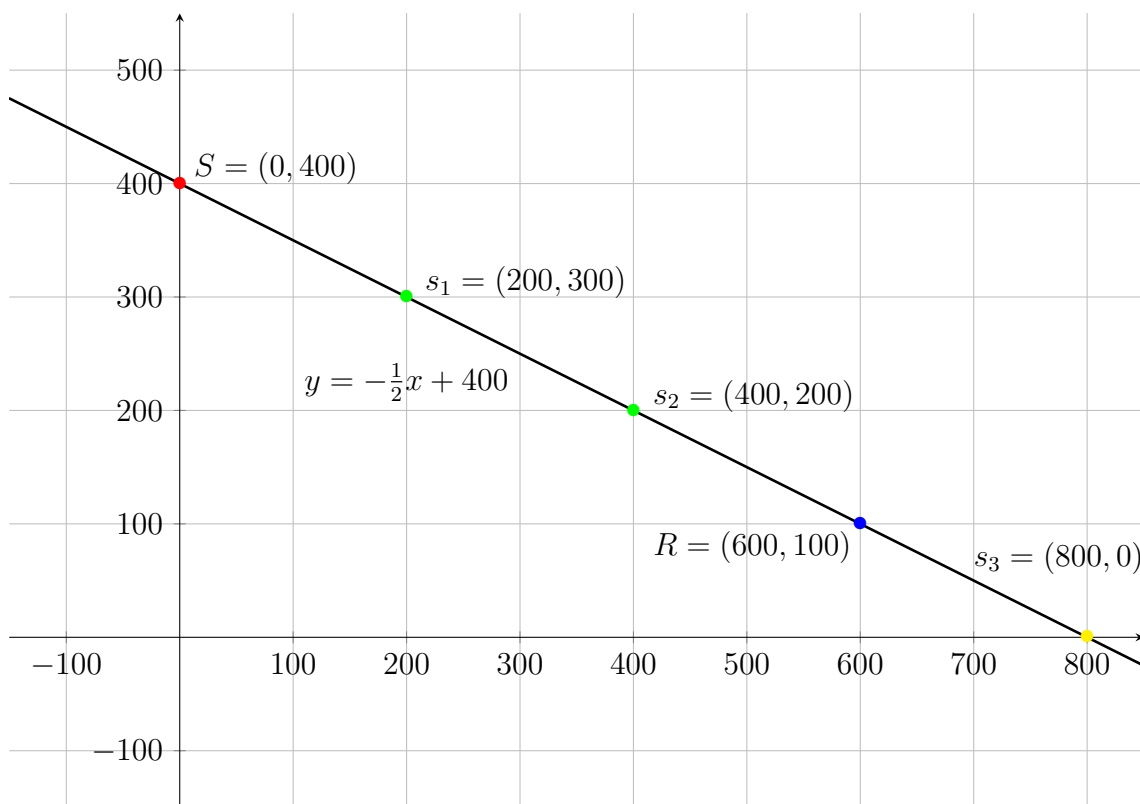


Abbildung 5: Erweiterung des Geheimnisses S als Gerade f für zwei Shares s_1 und s_2 .

Graphisches $(3, n)$ -Schema

Blah

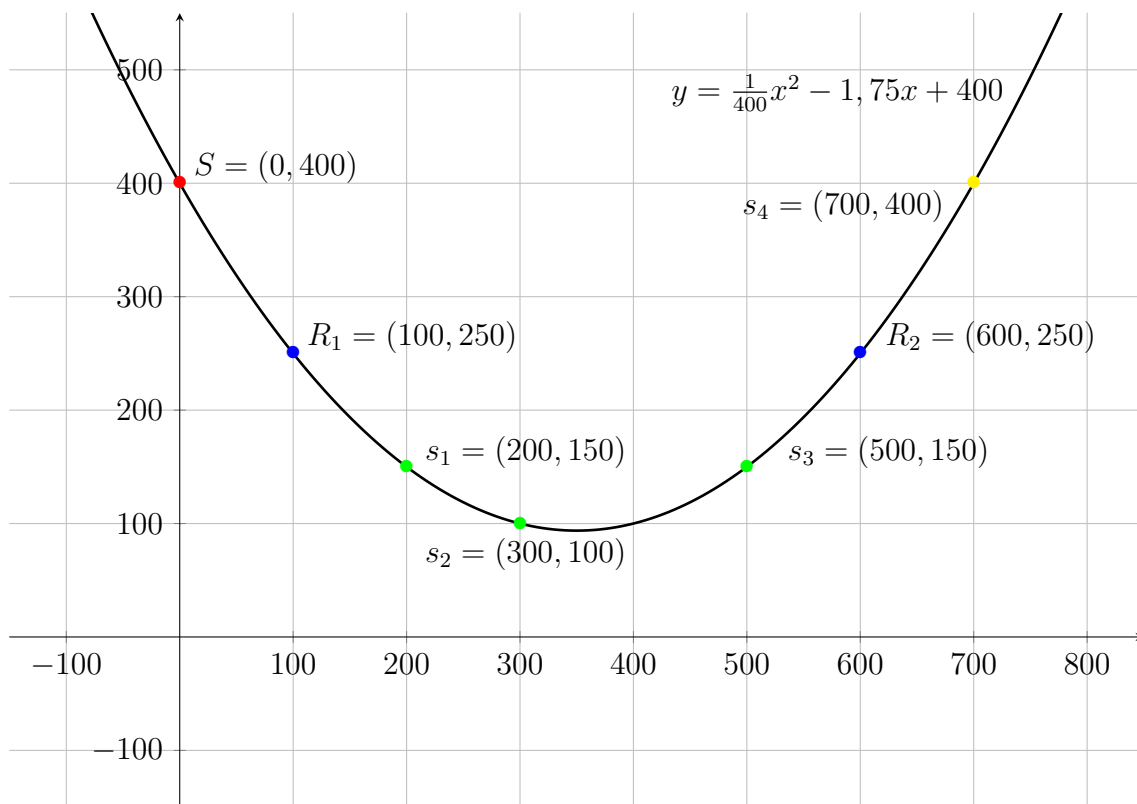


Abbildung 6: Parabel

4 Weitere Verfahren

Blah

4.1 Blakeley's

Blah

4.2 Chinesischer Restsatz

Blah

4.3 whatever...

Blah

5 Fazit

Abbildungsverzeichnis

1	Eine zufällige erste Folie. Von [2].	4
2	Berechnung der Pixel der zweiten Folie. Von [2].	4
3	Die zweite Folie. Von [2].	5
4	Das mittels beider Folien rekonstruierte Geheimnis. Von [2].	5
5	Erweiterung des Geheimnisses S als Gerade f für zwei Shares s_1 und s_2	8
6	Parabel	9

Literaturverzeichnis

- [1] BUCHMANN, J. *Einführung in die Kryptographie*. Springer Berlin Heidelberg, 2016.
- [2] KUHLEMANN, O. Visuelle Kryptografie. <http://kryptografie.de/kryptografie/chiffre/visuelle-kryptografie.htm>.
- [3] LIU, C. L. *Introduction to Combinatorial Mathematics*. McGraw-Hill, New York, 1968.
- [4] NAOR, M., AND SHAMIR, A. Visual cryptography. *Lecture Notes in Computer Science* (1995), 1–12.
- [5] SHAMIR, A. How to share a secret. *Communications of the ACM* 22, 11 (Nov 1979), 612–613.
- [6] SHANNON, C. E. Communication Theory of Secrecy Systems. *Bell System Technical Journal* 28, 4 (1949), 656–715.